Web Security III

Question 1 ***CSRF++***

Patsy-Bank learned about the CSRF flaw on their site described above. They hired a security consultant who helped them fix it by adding a random CSRF token to the sensitive `/transfer` request. A valid request now looks like:

```
https://patsy-bank.com/transfer?to=bob&amount=10&token=<random>
```

The CSRF token is chosen randomly, separately for each user.

Not one to give up easily, Mallory starts looking at the welcome page. She loads the following URL in her browser:

```
https://patsy-bank.com/welcome?name=<script>alert("Jackpot!");</script>
```

When this page loaded, Mallory saw an alert pop up that says "Jackpot!". She smiles, knowing she can now force other bank customers to send her money.

(a) What kind of attack is the welcome page vulnerable to? Provide the name of the category of attack.

Solution: Reflected XSS

(b) Mallory plans to use this vulnerability to bypass the CSRF token defense. She'll replace the `alert("Jackpot!");` with some carefully chosen JavaScript. What should her JavaScript do?

Solution: Load a payment form, extract the CSRF token, and then submit a transfer request with that CSRF token.

Or: Load a payment form, extract the CSRF token, and send it to Mallory.

(c) `patsy-bank.com` sets `SameSite=strict` for all of its cookies. Does this stop the attack from part (b)? Assume the welcome page does not require a user to be logged in.

Solution: Nope, because the malicious request will be sent from the welcome page of patsy-bank.com which is of the correct origin domain.

(d) Mallory wants to attack Bob, a customer of Patsy-Bank. Name one way that Mallory could try to get Bob to click on a link she constructed.

Solution: Send him an email with this link (making it look like a link to somewhere interesting). Post the link on a forum he visits. Set up a website that Bob will visit, and have the website open that link in an iframe. Send Bob a text message or a message on Facebook with the link.

(There are many possible answers.)

Question 2 ***Clickjacking***

In this question we'll investigate some of the click-jacking methods that have been used to target smartphone users.

(a) In many smartphone browsers, the address bar containing the page's URL can be hidden when the user scrolls. What types of problems can this cause?

> **Solution:** If the real address bar is hidden, it's much easier for an attacker to create and place their own on the website, fooling victims into thinking they're browsing on sites they aren't. JavaScript can scroll the page, hiding the address bar as soon as the page loads, allowing an attacker complete freedom to place a fake address bar.
>
> For more info, check out https://www.usenix.org/legacy/event/upsec/tech/full_papers/niu/niu_html/niu_html.html (section 4.2.2)

(b) Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

> **Solution:** By simulating an alert or popup on the website, an attacker can fool users into clicking malicious links. This can allow attackers to pose as phone applications such as texting apps or phone apps, which enables phishing.

(c) QR codes haven't taken off and become ubiquitous like some thought they would. Can you think of any security reasons why this might be the case?

> **Solution:** QR codes placed in public places are perfect targets for people with malicious websites. They can post their own, pretending to be links to useful websites, and instead linking to phishing sites. Or, they can modify and paste over existing codes, which only keen observers would notice.

Question 3 *Web Security Wrap-Up: UI-Based Attacks and Privacy*

(a) **Phishing**

A phishing attacker tries to gain sensitive user information by tricking users into going to a fake version of a website they trust. The attacker might convince the user to go to what *appears* to be their bank and to enter their username and password.

i. What are some ways that attackers try to fool users about the site they are going to? How do they convince people to click on links to sites?

ii. What are some defenses you should employ against phishing?

Solution:

i. Attacks include:

Sub domains that look like top level domains.

Look alike UNICODE urls: bankofamerca.com, bankofthevvest.com

Look alike unicode characters.

Mentioning recent information. Compromising an email account and then sending emails to people that account has recently corresponded with.

ii. Defenses include:

Use a browser-integrated password manager, it will automatically fail to fill in your password if the website is not legitimate.

Do not click on unexpected links in emails.

If your bank sends you an email about your account, go to your browser and separately type in the banks url, or call them. Do not click on links to sensitive sites that others provide you.

Type sensitive domains directly into the address bar, or create a short cut that way and then use it.

Some phishing emails or sites are not very well crafted. Subtle language or spelling errors, that should be out of place for the legitimate site, can be a warning sign that you should heed.

(b) **Clickjacking**

Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

Solution: By simulating an alert or popup on the website, an attacker can fool users into clicking malicious links. This can allow attackers to pose as phone

applications such as texting apps or phone apps, which enables phishing.

(c) **Web Tracking**

What kind of information do sites gain about you when you visit them? How could a business learn about many of the sites you visit and construct a detailed profile of you based on your web habits?

Solution: Technical information: the time of the request, your browser, OS, language, screen size, screen resolution, IP, and general location from your IP address.

What you requested: a search term, a news article.

The site also receives any cookies for that domain, allowing it to provide continuity of an activity that spans several pages, or required a login.

A business that provides ad analytics services can have client websites provide any information about you to the ad company as part of an image request. They can also plant and retrieve cookies associated with your identity any time you visit a client website, even if you never visit the ad company's website yourself.